IN THE CLAIMS

The claims are as follows:

1. (Previously Presented) A method of providing an authentication service, comprising:
with an authentication server, relating a user identity to a set of authentication mechanisms, the user identity belonging to a user;
relating a type of transaction with a relying party to a level of authentication, the relying party reliant on the authentication service to authenticate the user before user access is provided to its service, program or information;
the user or relying party selecting at least two authentication mechanisms to input from the set of authentication mechanisms according to the level of authentication associated with the type of transaction, the at least two authentication mechanisms selected from known secrets, stored secrets, biometrics and combinations thereof, wherein a flexible authentication process is provided; and
authenticating the user identity through the at least two authentication mechanisms, wherein the user is granted or denied access to the service, program or information provided by the relying party.

2. (Canceled)

3. (Original) The method as recited in claim 1, further comprising:
monitoring a series of authentications for the relying party to detect fraud.

4. (Withdrawn) The method as recited in claim 1, wherein the at least two authentication mechanisms in the set of authentication mechanisms are part of a distributed system.

5. (Previously Presented) The method as recited in claim 3, wherein the at least two authentication mechanisms are input to the authentication server with a mobile input device.

6. (Withdrawn) A computer-readable medium having computer-executable instructions for performing the method as recited in claim 1.

7. (Withdrawn) A method of syndication, comprising:

with an authentication server, offering an authentication service capable of authenticating a user identity from a selection of authentication mechanisms, the user identity belonging to a user;

the user or at least one relying party selecting at least two authentication mechanisms to input from the selection of authentication mechanisms, the at least two authentication mechanisms selected from known secrets, stored secrets, biometrics and combinations thereof, wherein a flexible authentication process is provided;

rendering results of the authentication to the at least one relying party, the at least one relying party reliant on the authentication service to authenticate the user before user access is provided to its goods or services;

dynamically making an authorization decision; and

distributing the authentication service to the at least one relying party wherein the at least one relying party provides or does not provide a good or service to the user depending on the authorization decision.

8. (Withdrawn) The method as recited in claim 7, wherein the at least one relying party integrates the authentication service together with other offerings.

9. (Withdrawn) The method as recited in claim 7, wherein the dynamic authorization decision is based on a requested access level, the at least two authentication mechanisms used, and an account status.

10. (Withdrawn) The method as recited in claim 7, further comprising:

providing secure recovery from potential fraud without requiring re-registration of the user.

11. (Withdrawn) The method as recited in claim 7, further comprising:

charging the relying party for each authenticating event.

12. (Withdrawn) A computer-readable medium having computer-executable instructions for performing the method as recited in claim 6.

13. (Withdrawn) A method of registration, comprising:

with an authentication server, authenticating a user having a user identity, wherein the user or a relying parts selects at least two mechanisms to input from a set of authentication mechanisms, the at least two authentication mechanisms selected from known secrets, stored secrets, biometrics and combinations thereof, wherein a flexible authentication process is provided;

determining a level of user identity confirmation for a registration;

selecting a new authentication mechanism for the user to send to the authentication server;

receiving the new authentication mechanism from the user;

receiving new authentication verification information;

storing user identity information, the level of identity confirmation, and the new authentication verification information in a database; and

sending the user identity information, the level of identity confirmation, and the new authentication verification information.

14. (Withdrawn) The method as recited in claim 13, wherein authenticating the user is done by a registration server.

15. (Withdrawn) The method as recited in claim 13, wherein authenticating the user is done by a registration agent.

16. (Withdrawn) The method as recited in claim 13, wherein authenticating the user is performed by using authentication mechanisms stored in the database.

17. (Withdrawn) The method as recited in claim 13, further comprising:
receiving from the user, a request for registration.

18. (Withdrawn) The method as recited in claim 17, wherein receiving the request for registration is done by an authentication server.

19. (Withdrawn) The method as recited in claim 17, wherein receiving the request for registration is done by an authentication agent.

20. (Withdrawn) The method as recited in claim 13, wherein determining the level of identity confirmation for the registration is done by a registration server.

21. (Withdrawn) The method as recited in claim 13, wherein determining the level of identity confirmation for the registration is done by a registration agent.

22. (Withdrawn) The method as recited in claim 13, wherein receiving new authentication verification information is done by a registration server.

23. (Canceled)

24. (Withdrawn) The method as recited in claim 13, wherein sending is done from a registration server to an authentication server.

25. (Withdrawn) The method as recited in claim 13, wherein sending is done from a registration agent to a registration server.

26. (Withdrawn) The method as recited in claim 13, further comprising sending pre-existing user information.

27. (Previously Presented) A method of providing an authentication service, comprising:

with an authentication server, providing a list of supported authentication methods to authenticate at least one user;

receiving requirements for an authentication level from at least one relying party, the at least one relying party reliant on the authentication service to authenticate the at least one user before user access is provided to its service, program or information;

receiving a selection of at least two authentication methods from the at least one user, the at least two authentication mechanisms selected from known secrets, stored secrets, biometrics and combinations thereof, wherein a flexible authentication process is provided and the selection can include a subset of the list of supported authentication methods;

receiving identification information for the at least one user;

producing a portfolio associated with the at least one user, the portfolio comprising the list of authentication methods, each authentication method in the portfolio meeting the selection of the at least one user, each authentication method in the portfolio supported by an authentication system, the list of authentication methods meeting the requirements for the authentication level from the at least one relying party; and

relating the identification information to the portfolio for the at least one user.

28. (Canceled)

29. (Withdrawn) The method as recited in claim 27, further comprising:

storing the portfolio on an authentication server capable of providing the authentication service to the at least one relying party.

30. (Withdrawn) The method as recited in claim 27, further comprising:
providing a selection of authentication methods to the at least one user;
receiving at least two selected authentication methods from the at least one user; and
receiving authentication information required to perform authentication for each of the at least two selected authentication methods, wherein the portfolio includes the authentication information.

31. (Withdrawn) The method as recited in claim 27, further comprising:
authenticating, by the authentication system, the at least one user to the at least one relying party.

32. (Withdrawn) The method as recited in claim 31, wherein authenticating the at least one user to the at least one relying party comprises:
providing at least two challenges to the at least one user;
accepting a response to each of the at least two challenges from the at least one user;
examining each of the responses to the at least two challenges to ensure their authenticity;
comparing authentication information received by the at least one user to the portfolio associated with the at least one user; and
communicating an authentication result to the at least one relying party.

33. (Withdrawn) The method as recited in claim 27, wherein the at least one relying party is an online pharmacy and the at least one user is a doctor.

34. (Withdrawn) The method as recited in claim 27, further comprising:
adding a new authentication method to the portfolio.

35. (Withdrawn) The method as recited in claim 34, wherein adding the new authentication method to the portfolio comprises:

authenticating the at least one user using an authentication method already in the portfolio;

receiving authentication information for the new authentication method; and

storing the new authentication method and its authentication information in the portfolio.

36. (Original) The method as recited in claim 27, further comprising:

receiving notice of a potentially compromised authentication method in the portfolio;

authenticating the at least one user using an authentication method already in the portfolio, but not using the potentially compromised authentication method; and

revoking the authentication information for the potentially compromised authentication method in the portfolio associated with the at least one user.

37. (Original) The method as recited in claim 27, further comprising:

monitoring authentication events for the at least one user; and

detecting possible fraud for a suspect authentication method.

38. (Original) The method as recited in claim 37, further comprising:

authenticating the at least one user using an authentication method already in the portfolio, but not using the suspect authentication method;

communicating the possible fraud to the at least one user; and

upon confirmation of fraud, revoking the suspect authentication method in the portfolio.

39. (Previously Presented) The method as recited in claim 37, further comprising:

automatically revoking the suspect authentication method in the portfolio, wherein the possible fraud is potentially serious fraud.

40. (Withdrawn) A computer-readable medium having computer-executable instructions for performing the method as recited in claim 27.

41. (Withdrawn) A method of authentication, comprising:

requesting, by a user to a relying party, a protected service;

sending, by the relying party, a description of the request to an authorization server;

determining, by the authorization server, a first level of assurance;

sending, by the authorization server to an authentication server, the first level of assurance;

requesting, by the authentication server, authentication from the user;

selecting, by the user or the relying party, at least two types of authentication information, the at least two authentication information selected from known secrets, stored secrets, biometrics and combinations thereof, wherein a flexible authentication process is provided;

entering, by the user, the at least two types of authentication information into an authentication device;

sending, by the authentication device to the authentication server, the at least two types of authentication information;

verifying, by the authentication server, the at least two types of authentication information using authentication verification information stored in a portfolio in a database that is associated with the user;

computing, by the authentication server, a second level of assurance;

evaluating whether the second level of assurance is high enough;

sending, by the authentication server to the authorization server, a first success message, upon determining the second level of assurance is high enough;

verifying, by the authorization server, information from the authentication server;

verifying, by the authorization server, that the user is allowed to perform the protected service;

sending, by the authorization server to the relying party, a second success message, upon verification of the at least two types of information from the authentication server and verification that the user is allowed to perform the protected service; and

providing, by the relying party to the user, the protected service.

42. (Withdrawn) The method as recited in claim 41, further comprising:

requesting, by the authentication server to the user, authentication using at least one additional authentication method, upon determining the second level of assurance is not high enough.

43. (Withdrawn) The method as recited in claim 42, further comprising:

sending, by the authentication server to the authorization server, a first failure message and a reduced level of assurance, upon determining the user is unable to authenticate using the at least one additional authentication method;

storing, by the authorization server, the reduced level of assurance;

sending, by the authorization server to the relying party, a second failure message; and

providing, by the relying party to the user, a third failure message.

44. (Previously Presented) The method of claim 1 wherein two or more authentication mechanisms are chosen.

45-47. (Canceled)

48. (Previously Presented) The method of claim 47 wherein at least one of the known secrets is interactive.

49-52. (Canceled)

53. (Withdrawn) The method of claim 27 wherein the at least one relying party is a laboratory or medical research facility or a health insurance company and the at least one user is a doctor.

54. (Withdrawn) The method of claim 27 wherein the at least one relying party is a stock exchange and the at least one user is a broker.

55. (Withdrawn) The method of claim 27 wherein the at least one relying party is a federal agency and the at least one user is an undercover agent.

56. (Previously Presented) The method of claim 1 wherein the known secret is selected from a password, identification number, family name, and combinations thereof.

57. (Previously Presented) The method of claim 1 wherein the stored secret is selected from a digital signature key, smart card, card containing a fixed secret, and combinations thereof.

58. (Previously Presented) The method of claim 1 wherein the biometric is selected from a fingerprint, retina, iris, palm print, facial structure, voice recognition, and combinations thereof.